ElSword LUAs Crypto Analisys

d3vil401 (http://d3vsite.org) - ESEmu Project (http://esemuproject.com)

First approach

By look at the benchmark of the files decryption and with a first look to the encryption algorithm we can consider the idea of a XOR or its variant.

Reverse Engineering it

OllyDRX

- Anti-Anti-Debuggers.
- Anti-Anti-Dumps.
- Themida unpacked target (x2.exe).
- Themida VM removed (x2.exe).
- d3vCrypto Script (ODBGScript).

Debug Trace (Routine Entry Point)

REGISTERS	VALUE	DESCRIPTION
EAX	0x00000000	*Key Pointer*
ECX	0x05F85E60	*Encrypted Buffer*
EDX	0x7FFD0000	*Differential XORer*
EBX	0x51A3F417	*UNKNOWN*
ESP	0x0018D79C	***S.P.*** -> *UNKNOWN*
EBP	0x000130E2	*Encrypted Buff Size*
ESI	0x0000000B	*Key Size*
EDI	0x05F85E60	*Encrypted Buffer*

Code

```
Decrypt:
movzx eax, byte ptr ss:[esp + esi + 0x118]
movzx ecx, bl
inc esi
dec ebp
xor eax, ecx
cmp esi, 0x14
jnz NoKeyReset
   xor esi, esi
NoKeyReset:
   mov edx, dword ptr ss:[esp + 0x34]
   mov cl, byte ptr ds:[edx + edi]
   mov edx, dword ptr ss:[esp + 0x3C]
   not cl
   movzx ecx, cl
   xor ecx, cl
   mov edx, dword ptr ds:[edx + ecx * 4]
   mov dword ptr ss:[esp + 0x24], edx
   xor al, byte ptr ss:[esp + 0x24]
   and edx, 0xFFFFFF00
   or edx, ecx
   shr ebx, 0x8
   mov byte ptr ds:[edi], al
   inc edi
   xor ebx, edx
   test ebp, ebp
   jnz Decrypt
```

IDA

```
If (KeyCounter > 20)
  KeyCounter %= 20;
do
{
   KeyByte = Key[KeyCounter++];
   --KeySize;
   v31 = v8 ^ KeyByte;
   if (v10 == 10)
      v10 = 0;
   v27 = v31 ^ ~*(v224 + v29);
   v220 = *(v226 + 4 * v27);
   v33 = v27 / v220 & 0xFFFFFF00;
   v29++ = v220 ^ v31;
   v8 = v33 ^ (v8 >> 8);
} while (v28);
```

Mathematical Analisys

Variables identifications

EAX	*MK*	1028 Bytes Key
EBP	*D*	Encrypted Buffer
ESI	K_I	Key Index
EDI	K_s	Static Key Size
STATIC	D_c	Buffer Counter

Decryption

$$\sum_{K_i < 20}^{K_i = 0} \left((D[D_c])^{\wedge}((Key[K_i])^{\wedge}(D[D_c]^{\wedge}Key[K_i]) \right)$$

Key Generation